Note: The following appendix will not appear in the Code of Federal Regulations

Addendum 1

HIPAA SECURITY MATRIX

Please Note: (1) While we have attempted to categorize security requirements for ease of understanding and reading clarity, there are overlapping areas on the matrix in which the same requirements are restated in a slightly different context. (2) To ensure that no Requirement or Implementation feature is considered more important than another, this matrix has been presented, within each subject area, in alphabetical order.

ADMINISTRATIVE PROCEDURES TO GUARD DATA INTEGRITY, CONFIDENTIALITY, AND AVAILABILITY

REQUIREMENT:	IMPLEMENTATION:
Certification	
Chain of trust partner agreement	
Contingency plan (all listed implementation features must be implemented).	Applications and data criticality analysis. Data backup plan. Disaster recovery plan. Emergency mode operation plan. Testing and revision.
Formal mechanism for processing records.	
Information access control (all listed implementation features must be implemented).	Access authorization. Access establishment. Access modification.
Internal audit	
Personnel security (all listed implementation features must be implemented).	Assure supervision of maintenance personnel by authorized, knowledgeable person. Maintenance of record of access authorizations. Operating, and in some cases, maintenance personnel have proper access authorization. Personnel clearance procedure. Personnel security policy/procedure. System users, including maintenance personnel, trained in security.

Security configuration mgmt. (all listed implementation features must be implemented).	Documentation. Hardware/software installation & maintenance review and testing for security features. Inventory. Security Testing. Virus checking.
Security incident procedures (all listed implementation features must be implemented).	Report procedures. Response procedures.
Security management process (all listed implementation features must be implemented).	Risk analysis. Risk management. Sanction policy Security policy.
Termination procedures (all listed implementation features must be implemented).	Combination locks changed. Removal from access lists. Removal of user account(s). Turn in keys, token or cards that allow access.
Training (all listed implementation features must be implemented)	Awareness training for all personnel (including mgmt). Periodic security reminders. User education concerning virus protection. User education in importance of monitoring log in success/failure, and how to report discrepancies. User education in password management.

PHYSICAL SAFEGUARDS TO GUARD DATA INTEGRITY, CONFIDENTIALITY, AND AVAILABILITY

REQUIREMENT:	IMPLEMENTATION:
Assigned security responsibility	
Media controls (all listed implementation features must be implemented).	Access control. Accountability (tracking mechanism). Data backup. Data storage. Disposal.
Physical access controls (limited access) (all listed implementation features must be implemented).	Disaster recovery. Emergency mode operation. Equipment control (into and out of site).

	Facility security plan. Procedures for verifying access authorizations prior to physical access. Maintenance records. Need-to-know procedures for personnel access. Sign-in for visitors and escort, if appropriate. Testing and revision.
Policy/guideline on work station use	
Secure work station location	
Security awareness training	

TECHNICAL SECURITY SERVICES TO GUARD DATA INTEGRITY, CONFIDENTIALITY, AND AVAILABILITY

REQUIREMENT:	IMPLEMENTATION:
Access control (The following implementation feature must be implemented: Procedure for emergency access. In addition, at least one of the following three implementation features must be implemented: Context-based access, Role-based access, User-based access. The use of Encryption is optional).	Context-based access. Encryption. Procedure for emergency access. Role-based access. User-based access.
Audit controls	
Authorization control (At least one of the listed implementation features must be implemented).	Role-based access. User-based access.
Data Authentication	
Entity authentication (The following implementation features must be implemented: Automatic logoff, Unique user identification. In addition, at least one of the other listed implementation features must be implemented).	Automatic logoff. Biometric. Password. PIN. Telephone callback. Token. Unique user identification.

TECHNICAL SECURITY MECHANISMS TO GUARD AGAINST UNAUTHORIZED ACCESS TO DATA THAT IS TRANSMITTED OVER A COMMUNICATIONS NETWORK

REQUIREMENT:	IMPLEMENTATION:
Communications/network controls (The following implementation features must be implemented: Integrity controls, Message authentication. If communications or networking is employed, one of the following implementation features must be implemented: Access controls, Encryption. In addition, if using a network, the following four implementation features must be implemented: Alarm, Audit trail, Entity authentication, Event reporting).	Access controls. Alarm. Audit trail. Encryption. Entity authentication. Event reporting. Integrity controls. Message authentication.

ELECTRONIC SIGNATURE

REQUIREMENT:	IMPLEMENTATION:
Digital signature (If digital signature is employed, the following three implementation features must be implemented: Message integrity, Non-repudiation, User authentication. Other implementation features are optional.)	Ability to add attributes. Continuity of signature capability. Countersignatures. Independent verifiability. Interoperability. Message integrity. Multiple Signatures. Non-repudiation. Transportability. User authentication.